TRUSTONIC

<t-base-300 for MT6582

<mark>**Early Access Version**</mark>

Release Notes

<t-base

TABLE OF CONTENTS

1 INTRODUCTION

This document contains the Release Notes for the <t-base product on Mediatek MT6582 platform.

The version of the product is <t-base-300 V003 Early Access.

<mark>WARNING: this version has not been fully validated and is not ready for production.</mark>

2 WHAT'S NEW?

2.1 <T-BASE 300 V001 (EARLY ACCESS)

Initial <t-base integration allowing Android boot on CPU0 in normal world (replacing Mediatek's FakeTEE).

2.2 <T-BASE 300 V002 (EARLY ACCESS)

Changed IRQ used to notify NWd from SWd to be IRQ 80 (Shared Peripheral Interrupt).

Using software crypto driver instead of empty stubs as initially done (as it allows for primary validation while crypto driver development is done in parallel).

2.3 <T-BASE 300 V003 (EARLY ACCESS)

This early access v3 of t-base is now able to executing trusted applications and secure drivers .

It also adds:

- SMP boot of Android.
- Power schemes supported: CPU hotplug of secondary cores.
- HW RNG integration done.

2.4 <T-BASE 300 V004 (EARLY ACCESS)

The early access v4 includes:

- Fix to support handling of multiple interrupts in one secure driver.
- Extension of virtual memory available for HW mapping (until 16MB).
- Partial support of CPU 0 Dormant mode.

3   SYSTEM REQUIREMENTS

3.1 HARDWARE

Mediatek MT6582 devices.

3.2 SOFTWARE FOR DEVELOPER PC

SW Components & Tools	Source	Version
Operating System (including service pack):		Windows XP SP3 32bit, Ubuntu 12.04 64bit
Android NDK	Google	r7b
ARM RVCT	ARM	4.1
Android images	Mediatek	BSP images, release 20131007, with patches
Linux Kernel	Mediatek	Kernel images, release 20131007, with patches

4 KNOWN ISSUES

There is no known issue